Introduction to Data Privacy Law in Malaysia

Data Privacy Law in Malaysia – The Personal Data Protection Act ("**PDPA**") which came into force on 15 November 2013 is enacted to regulate the processing of personal data in commercial transactions only and does not apply to the federal nor state government.

Data User and Data Processor

A 'data user' is defined under the PDPA as a person who processes any personal data or has control over or authorizes the processing of any personal data, but does not include a 'data processor'.

Under the PDPA, the term 'processing' includes collecting, recording, holding or storing the personal data.

A 'data processor' is defined under the PDPA as any person, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes. It does not include an employee of the data user.

Scope of Personal Data

Any information may be considered as personal data under data privacy law in Malaysia if a specific individual is identified or identifiable from that information or from that information and other Information in the possession of the data user. Hence, anonymised data, being data converted into a form which does not identify individuals, would not fall within the definition of "personal data.

Data Protection Principles

The data protection principles under the PDPA (the "**Data Protection Principles**") as set out below are imposed upon the "data user" and *not* on the "data processor". However, a data processor may also be liable under data privacy law in Malaysia if personal data is unlawfully disclosed to a third party without the consent of the data user.

- General Principle – The General Principle requires that personal data of a data subject should only be processed if consent has been obtained unless exempted by the PDPA. The consent to be obtained pursuant to the General Principle may be in any form as long as such consent can be recorded and maintained properly by the data user.
- Notice and Choice Principle – A data user must inform a data subject by written notice ("Privacy Notice") that the data subject's personal data is being processed by or on behalf of the data user. Other information that must be provided in the Privacy Notice includes the purpose of processing and the classes of third parties to whom the data user discloses or may disclose the personal data.
- Disclosure Principle – The Disclosure Principle provides that there should be no disclosure of personal data for any other purpose than for the purpose it was to be disclosed at the time of collection, or for purposes directly related to such purpose, or to any third party not provided for under the Privacy Notice, without the consent of the data subject.
- Security Principle – The Security Principle requires that a data user to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. Further, a data user is required to ensure that a data processor processing

personal data on its behalf provides sufficient guarantees in respect of technical and organisational security measures and measures governing the processing of personal data, and takes reasonable steps to ensure compliance with those measures.

- Retention Principle – The Retention Principle provides that personal data should not be kept longer than necessary for the fulfilment of the purpose of processing. Data users should take steps to ensure that personal data is destroyed or permanently deleted where it is no longer required.
- Data Integrity Principle – Under the Data Integrity Principle, a data user must take reasonable steps to ensure that personal data is accurate, complete, not misleading and kept-up-to-date.
- Access Principle – The Access Principle provides that a data subject shall be given access to his personal data held by a data user and be able to correct that personal data unless compliance with such a request to access or correct is refused in circumstances expressly set out under the PDPA.

Registration under PDPA

Under the Personal Data Protection (Class of Data Users) Order 2013 (the "**Order"**), certain classes of data users (including those in the telecommunications, banking and financial services sectors) are required to register with the PDP Commissioner and to obtain a certificate of registration. This requirement serves as a means for the PDP Commissioner to consistently monitor sectors that deal with large amounts of personal data. As the certificate of registration is valid only for a determined period and in order to maintain continuous and valid registration, a data user would have to ensure that it is in compliance with the PDPA, as a breach of any provision of the PDPA could result in the PDP Commissioner refusing to renew or revoking the registration of the said data user.